

## UNITED STATES DISTRICT COURT

for the  
Eastern District of TennesseeIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)A DELL COMPUTER CURRENTLY LOCATED AT THE  
FBI KNOXVILLE FIELD OFFICE, 1501 DOWELL  
SPRINGS BLVD, KNOXVILLE, TNCase No. 1:24-MJ- 16

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein.

located in the Eastern District of Tennessee, there is now concealed (identify the person or describe the property to be seized):

See, Attachment B hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(5)	Damaging a Protected Computer

The application is based on these facts:  
See, Affidavit of FBI SA Jeremy P. Allman

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/ Jeremy P. Allman

Applicant's signature

Jeremy P. Allman, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
video conference (specify reliable electronic means).

Date:

January 24, 2024City and state: Chattanooga TN

Judge's signature

Hon. Christopher Steger, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TENNESSEE  
AT CHATTANOOGA

IN THE MATTER OF THE SEARCH OF A  
DELL COMPUTER, CURRENTLY  
LOCATED AT THE FBI'S KNOXVILLE  
FIELD OFFICE, 1501 DOWELL SPRINGS  
BOULEVARD, KNOXVILLE, TENNESSEE

Case No. 1:24-mj- **16**  
Magistrate Judge Steger

**ATTACHMENT A**

The property to be searched is a Dell Precision 7200, service tag  
FT0JPY2, VC property number 691550 (the "Device").

The Device is currently located at the FBI's Knoxville Field Office, 1501 Dowell Springs  
Boulevard, Knoxville, Tennessee.

This warrant authorizes the forensic imaging and search of the Device for the purpose of  
identifying and seizing the electronically stored information described in Attachment B.

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TENNESSEE  
AT CHATTANOOGA

IN THE MATTER OF THE SEARCH OF A  
DELL COMPUTER, CURRENTLY  
LOCATED AT THE FBI'S KNOXVILLE  
FIELD OFFICE, 1501 DOWELL SPRINGS  
BOULEVARD, KNOXVILLE, TENNESSEE

Case No. 1:24-mj- 16  
Magistrate Judge Steger

**ATTACHMENT B**

All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1030(a)(5) since September 22, 2023, including:

- a. recently accessed files to include but not limited to document, files, pictures, and folders;
- b. any information related to files that were altered and/or modified between September 22, 2023 and September 29, 2023 to include but not limited to document, files, pictures, and folders;
- c. any information related to files that were deleted between July 1, 2023 and September 29, 2023 to include but not limited to document, files, pictures, and folders;
- d. any information related to login passwords, password change history, remote access, removable media, login banner;
- e. any information related to internet history, firewall logs, caches, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, downloaded files from the Internet, and records of user-typed web addresses installed;
- f. any information related to communication software, encrypted documents or containers;
- g. any information related file transport software and history;

- h. Powershell, Command Line, Jump List, and Registry Artifacts;
  - i. Records of user activity for any connections made to or from the Device, including the date, time, length, and method of connections, data transfer volume, username, and source or destination IP addresses.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, event logs, and browsing history;
3. Records evidencing the use of the remote access to the device from an unknown location.
4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TENNESSEE  
at CHATTANOOGA

IN THE MATTER OF THE SEARCH OF A  
DELL COMPUTER, CURRENTLY  
LOCATED AT THE FBI'S KNOXVILLE  
FIELD OFFICE, 1501 DOWELL SPRINGS  
BOULEVARD, KNOXVILLE, TENNESSEE

Case No. 1:24-mj-00016  
Magistrate Judge Steger

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeremy P. Allman, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been employed by the FBI since January 2016. I was a law enforcement officer in the State of Tennessee for approximately 14 years. For approximately six years, I was assigned to the Internet Crimes Against Children Task Force. During this time, I received training specifically designed to conduct internet-based investigations. Furthermore, I received training in the field of digital forensics. Since June 2016, I have been assigned to the FBI's Cyber Crime Task Force in Knoxville, Tennessee, as a Special Agent. As a Special Agent, I am authorized to investigate

violations of law of the United States, and I am a Special Agent with the authority to execute search warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violation of 18 U.S.C. § 1030 (a)(5) (Damaging a protected computer) has been committed by Employee 1. There is also probable cause to search and seize the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

5. The property to be searched is a Dell Precision 7200, service tag FT0JPY2, VC property number 691550 (the “Device”).

6. The Device is currently located at the FBI’s Knoxville Field Office, 1501 Dowell Springs Boulevard, Knoxville, Tennessee.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

### **PROBABLE CAUSE**

8. The United States is investigating an unauthorized access to a protected research computer system, i.e., the Device, owned by an educational institution, (the Victim Company, or “VC”), located in Knoxville, Tennessee.

9. On October 3, 2023, Task Force Officer (“TFO”) Kelley Kain and your affiant made contact with an information systems network administrator (“Complainant”) with VC. The Complainant stated a former employee (“Employee 1”) – whose identity is known to the FBI and to VC – gained unauthorized access to the Device owned by the VC. Employee 1 used the Device while employed at the VC. According to the Complainant, Employee 1 was the only person to use the Device while he was employed at the VC.

10. In late July or early August, Employee 1 left the VC and began working as a researcher at an educational institution in Texas. While employed at the VC, Employee 1 received two research grants, and the associated research publications were not complete at the time Employee 1 left the VC.

11. The Complainant was made aware on September 22, 2023, Employee 1 gained unauthorized remote access to the Device, owned by the VC, and maintained unauthorized access to the Device until September 28, 2023. Complainant advised that the password to the device was changed at some point after Employee 1’s termination. That change was done without authorization by the VC and was not undertaken by anyone at the VC with authorization to access the device or modify the password. Employee 1 was the only other individual who used the Device. The Device was taken offline on September 28, 2023. The Complainant took

custody of the Device on September 29, 2023, and maintained custody of the Device until providing the Device to the FBI.

12. According to the Complainant, the Device was not accessed since it was taken offline on September 28, 2023. On October 3, 2023, the Complainant released custody of the Device and voluntarily provided the Device to TFO Kain and your affiant. On October 3, 2023, the Complainant gave written consent, via FBI consent-to-search form, to search the Device.

13. The Complainant was not aware of what is stored on the Device or Employee 1's actions while remoted in the Device besides changing the password. The Complainant could not identify what was accessed, altered, modified, and/or deleted on the Device. It was unknown to the Complainant whether there were files on the Device that ~~Employee 1~~ <sup>were CHS</sup> beyond the scope of Employee 1's access permissions while he was employed at the VC. The Complainant indicated his/her belief that someone at the VC may have provided Employee remote access without authorization. Neither the Complainant nor the VC has indicated to me that the VC has confirmed how Employee 1 obtained access to the Device. However, at the time he changed the password on the Device, Employee 1 did not have VC's permission to access the device or its contents, change any user or password information, or otherwise interact with the Device in any capacity.

14. On October 31, 2023, TFO Kain met with General Counsel for the VC. General Counsel stated that VC would feel more comfortable if the FBI would seek a search warrant in lieu of consent. Accordingly, FBI is treating the consent previously granted as revoked. The VC is aware that FBI maintains possession of the device and anticipates applying for the instant search warrant.



15. At some point prior to October 31, 2023, a Computer Forensic Examiner with the FBI's Computer Analysis Response Team used forensic tools to create a partial forensic image of the Device's hard drives. Digital forensic examination did not occur during the imaging process and has not occurred prior to this search warrant application.

16. The Device is currently in lawful possession of the FBI and in storage at Evidence Control Room at the FBI's Knoxville Field Office, 1501 Dowell Springs Boulevard, Knoxville, Tennessee. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI. Though the Device was originally partially imaged pursuant to the initial written consent of Complainant, the imaging process was not completed. I now seek this warrant to allow FBI to generate and search a complete forensic image of the Device and all its contents.

#### **TECHNICAL TERMS**

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. "Digital device," as used herein, includes the following terms and their respective definitions:

1. A "computer" means an electronic, magnetic, optical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in

conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2. “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.”
3. “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not

limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).”

- b. IP Address (“IP”) An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address (in a format referred to as “IPv4” formatting) is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). IP addresses in the “IPv6” protocol serve a similar function but contain various alphanumeric values separated by colons. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data.

Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- e. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption

algorithm that usually requires a secret decryption key, to which adversaries do not have access.

- g. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

### **COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS**

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device. Recovery of this data

requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.



21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

#### **METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

23. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a

result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

- b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.
- c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence

of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

- d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot

be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

- e. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

24. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

- a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of

the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

- b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.
- c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

### CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

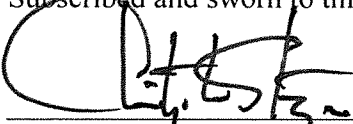
Respectfully submitted,

/s/ Jeremy P. Allman

Jeremy P. Allman  
Special Agent, Federal Bureau of  
Investigation

In accordance with Fed. R. Crim. P. 4.1(b)(2)(A), the affiant attested under oath the contents of this affidavit, which was submitted to by reliable electronic means.

Subscribed and sworn to this 24 day of January, 2024.



Hon. Christopher H. Steger,  
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF A  
DELL COMPUTER, CURRENTLY  
LOCATED AT THE FBI'S KNOXVILLE  
FIELD OFFICE, 1501 DOWELL SPRINGS  
BOULEVARD, KNOXVILLE, TENNESSEE

Case No. 1:24-mj-**00016**  
Magistrate Judge Steger

**ATTACHMENT A**

26. The property to be searched is a Dell Precision 7200, service tag FT0JPY2, VC property number 691550 (the "Device").

The Device is currently located at the FBI's Knoxville Field Office, 1501 Dowell Springs Boulevard, Knoxville, Tennessee.

This warrant authorizes the forensic imaging and search of the Device for the purpose of identifying and seizing the electronically stored information described in Attachment B.

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF A  
DELL COMPUTER, CURRENTLY  
LOCATED AT THE FBI'S KNOXVILLE  
FIELD OFFICE, 1501 DOWELL SPRINGS  
BOULEVARD, KNOXVILLE, TENNESSEE

Case No. 1:24-mj-**00016**  
Magistrate Judge Steger

**ATTACHMENT B**

All records on the Device described in Attachment A that relate to violations of 18 U.S.C.

§ 1030(a)(5) since September 22, 2023, including:

- a. recently accessed files to include but not limited to document, files, pictures, and folders;
- b. any information related to files that were altered and/or modified between September 22, 2023 and September 29, 2023 to include but not limited to document, files, pictures, and folders;
- c. any information related to files that were deleted between July 1, 2023 and September 29, 2023 to include but not limited to document, files, pictures, and folders;
- d. any information related to login passwords, password change history, remote access, removable media, login banner;
- e. any information related to internet history, firewall logs, caches, cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into



any Internet search engine, downloaded files from the Internet, and records of user-typed web addresses installed;

- f. any information related to communication software, encrypted documents or containers;
- g. any information related file transport software and history;
- h. Powershell, Command Line, Jump List, and Registry Artifacts;
- i. Records of user activity for any connections made to or from the Device, including the date, time, length, and method of connections, data transfer volume, username, and source or destination IP addresses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, event logs, and browsing history;

3. Records evidencing the use of the remote access to the device from an unknown location.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.